Key-note paper presented on the EHPG meeting of the OECD Halden Reactor Project, Storefjell, Norway, 12-15 March 2007.

Safety of nuclear power; the case for I&C and HF engineering

Björn Wahlström
Technical Research Centre of Finland (VTT)
+358 20 7226400, +358 20 7227046, bjorn.wahlstrom@vtt.fi

Abstract

The safety of nuclear power builds on many scientific and technical areas of which instrumentation and control (I&C) and human factors (HF) have shown to be very important. The OECD Halden Reactor Project (HRP) has been involved in these two areas for many years in their man-technology-organisation (MTO) research. In the view of a revival of nuclear power for electricity generation presently taking place, the MTO research and development (R&D) at HRP is growing in importance. The present paper discusses some of the challenges that can be seen in the fields of I&C and HF engineering and it concludes by stressing the importance for HRP to engage in dialogues with their signatories on needs and opportunities for new research in the MTO area. Such needs and opportunities should be integrated in the strategic considerations for the next three year programme of HRP that now is in its planning stage.

1. INTRODUCTION

Nuclear power is used for electricity production in 30+ countries [1]. The nuclear reactors have so far produced more than 50000 TWh and they have thus an important position in the electricity supply of the world. Nuclear power is however a controversial technology and several countries have declared that they will phase out their nuclear power plants. In Europe a different route has been taken by Finland, where a new reactor is being built. The new Finnish nuclear power plant is planned to start its commercial operation in 2010.

The societal acceptability of nuclear power depends crucially on actual and perceived safety of the plants. The two accidents of Three Mile Island and Chernobyl gave demonstrations both to the industry and to the public that safety cannot be compromised. A closer examination of these two accidents points to the importance of instrumentation and control (I&C) as well as human factors (HF) in ensuring safety of nuclear power. In the future it is expected that the importance of these two areas will grow due to an increasing number of modernisations of present plants and also due to new plants to be built.

The OECD Halden Reactor Project (HRP) has had, and is also in the future expected to have, an important position in the research of the two neighbouring fields of I&C and HF. It is therefore interesting to ask what needs and opportunities for new research could be seen in the two fields. This paper has been written with the intent to give the HRP an outsiders view on promising ideas for the years to come.

2. A REVIVAL OF NUCLEAR POWER

Nuclear power in the world is experiencing signs of a renaissance. The European Commission has for example in response to an increasing demand of imported energy and the need to decrease CO_2 emissions taken a positive view towards the use of nuclear power for electricity generation [2]. A recent plan to build a global nuclear energy partnership from the USDOE indicates a governmental interest in new nuclear power plants to be built in the US [3].

The revival of nuclear power within the industry is seen as a growing interest in modernising present plants. Many of the 440+ plants in the world were built with an assumption of 30-40 years of operational life, but today it is very clear that their technical lifetime is much longer. In the US nearly 50 plants have completed their application for an additional 20 years of operation and nearly 40 plants more are expected to follow [4]. In Europe similar trends also include power upgrades.

The costs of generated electricity will be one of the main factors influencing the willingness of utility companies to invest in nuclear power. In general nuclear power seems to be able to compete favourably with other energy sources [5], but actual costs will depend on the time it takes to build a new nuclear power plant and the load factor it will achieve.

3. BUILDING SAFETY INTO NUCLEAR POWER PLANTS

The construction of safety in the nuclear industry relies on two important principles, *defence in depth* and the protection against threats using *independent safety barriers*. The application of these principles leads to the introduction of *redundancy*, *diversity* and *separation* as well as the so called *30-minutes rule*, which ensure that no single equipment failure or human error will pose a threat to safety. I&C as well as the operators in the control room have the important tasks of ensuring that this safety principle is maintained.

3.1 Instrumentation and control

I&C is used to monitor and control major process components such as the reactor, the turbine and the generator as well as safety and auxiliary systems. Important safety systems are for example emergency core cooling, residual heat removal and systems to ensure containment integrity. Well functioning I&C systems are essential for a continued safety and availability of the plant. I&C encompass a large range of equipment such as sensors, transmitters, cabling, controllers, displays, control elements, servers, routers, etc.

Modern I&C systems are computer based, where a large range of equipment collect information, execute control algorithms and send control actions to pumps, valves and other equipment. Communication between the computers relies on high speed data highways and a common practice is that all process information is collected to a central data base, which may contain many ten thousand variables. The process database serves many different information needs such as control and performance calculations, display of process variables, alarming, trending, remote monitoring, etc.

The I&C in present operating nuclear power plants is however mostly not based on computers, but on analogue technology and relays. This means that plants in their modernisations projects are forced to bring in a new technology and this endeavour has presented hurdles in both implementing and licensing I&C [6]. The main difficulty in applying computer based I&C systems is connected to the burden of proof in demonstrating that the systems will include all intended, but no unintended functions.

The difficulty of ensuring safety of the I&C software is caused by its complexity. An I&C platform on which typical applications are built can easily contain millions of lines of code, which makes it impossible to test all possible paths through the software. From a licensing point of view it is therefore possible that some undetected software error may have disastrous consequences when an important function is needed. Unfortunately this problem can not be remedied by the use of redundancy or diversity, because the software error may have its root in the software specifications, which implies that the error is distributed to all copies and versions of the software in consideration.

3.2 Human factors

The importance of HF was identified in the Three Mile Island accident, where the major cause of the accident was attributed to poor control room design, deficient procedures and inadequate operator training. Today a considerable amount of guidance has been created to support control room design and the writing of procedures. This development has improved the situation, but the guidance has mostly been directed to improvements in the old technology.

The crucial task in designing computer based control rooms is to decide on how displays should be structured and on how they should present information for the operators. A common approach has been to integrate process information into mimic diagrams and to use colour coding to display attributes connected to components and variables. The mimic diagrams are also used for control by addressing plant objects e.g. with a mouse. One problem with addressable controls is that they can make operations slow and awkward, if they have not been designed properly. Alarm systems is another area, which have shown to be difficult to implement, in spite of the fact that computer based systems have a large potential for advanced functionality.

The effort needed in proving that some human system interface (HSI) is good enough has shown to be extensive. Is it for example necessary to build a fully functional simulator, or is it possible collect evidence on acceptability with part task simulation and mock-ups. The difficulty of finding subjects to take part in validation experiments and to train them has also shown to be excessive. Finally the number of scenarios needed to do a convincing control room validation has shown to raise controversies.

4. CHALLENGES WITHIN INSTRUMENTATION AND CONTROL

The main challenge today in applying modern instrumentation and control systems to nuclear power plants is to be able to provide convincing proofs that the software is good enough. Broadening this view there are however many other challenges that warrant R&D efforts. These are considered more in detail below.

4.1 Adapting to a rapid technical development

One large challenge for the nuclear power plants is to adapt their I&C systems to the short product lifetimes, which today are seen within computers and software. In this area one may distinguish between the following problems

- there is no product support when such would be needed,
- the company that supplied the original equipment has disappeared from the market,
- components and spare parts cannot be found on the market or they are very expensive,
- know-how in the technology base has disappeared,
- education in the old technology is not offered anymore.

The projected lifetime for a new plant today is sixty years and for computers and software perhaps between three and five years. I&C vendors may promise support for about twenty years, but that would still imply a need for two major I&C modernisations during the life of a plant.

The large difference in lifetime between nuclear power plants and I&C systems enforces plants to plan for upgrades and modernisations already when brand new equipment is installed. An attractive path would be to ensure a high re-usability of present designs and code in the I&C systems that are to be installed in the future. How such reusability could be ensured is not clear and would most likely have to build on new architectures and solutions.

4.2 Ensuring software quality

The most important challenge in ensuring software quality lies in innovative applications of risk assessment and safety engineering for computer based systems [7]. It is evident that a combination of deterministic and probabilistic reasoning has to be used, but before usable methods and tools have been developed considerable R&D efforts are needed.

One important part in achieving software quality is to develop better methods for reasoning about requirements, claims and evidence. Another part would be to create automated tools for the analysis of software modules. Software designs to support testability would also be important in ensuring software quality. For high reliability functions, such as reactor protection, it seems necessary to give reliability estimates for the software. Operational experience from some piece of software can provide evidence of quality, but today there are no agreed views on how this could be done. Finally accurate design records can help in establishing confidence in software, but how this should be done is an open question.

Nuclear power has never had the luxury of being able to use trial and error. Products delivered to nuclear power plants therefore have to be right from the beginning. More generally this implies a broad application of model based design methods and tools to make it possible to test designs virtually before they are moved to practical installations.

4.3 Common cause failures

The possibility of common cause failures is the major objection against the use of software based systems in nuclear power plants. The problem is very concrete, which can be seen from software error reports [8]. To some extent this problem can be approached by better software design processes and by a controlled use of redundancy and diversity. A final solution can only be solved by providing some assessment of the likelihood that execution paths in two or more redundant channels will hit the same software error simultaneously.

Risk informed arguments can use evidence from the software architecture, source code, testing activities and stochastic differences in input data to show that the likelihood for a CCF is very small. If this likelihood is compared with increased risks of operational and maintenance errors and it is combined with the possibility that a diverse channel may be triggered spuriously, the bottom line may be that diversity is inferior as compared with redundancy.

Another scenario is that a very large number of simple devices (time relays, motor protection, signal conditioning, etc.) with embedded computers running the same software would fail simultaneously. The possibility that a large number of such devices would have latent errors in their software cannot be excluded, but a thorough monitoring of such devices should at least in principle make it possible to detect unexpected behaviour. An accurate configuration and modification management should make it possible to minimise the risk of CCFs also for these applications.

4.4 Utilising the potentials of the technology

The perhaps most interesting challenge for R&D is to search for innovative ways to utilise the potentials of new I&C technology [9]. Reasons for adopting new technology can be found in the following arguments

- new technology offers functionality for improved safety and availability,
- obsolescence is forcing plants to modernise, i.e. a transfer to new technology,
- the business volume within computers and software is a driver of innovations and technological development that provides interesting applications also for the nuclear field,
- new technology offers the most cost efficient or perhaps even the only realistic alternative.

Opportunities of new technology include, but are not restricted to, improved data handling and computational structures, smarter hardware and software architectures, new algorithms, better trending, etc. Development in hardware is expected to provide increased computer speeds, larger bandwidths on communication highways and decreasing cost for information storage. This development of hardware and software performance may however also carry the drawback of increased system complexity.

There is a mounting pressure to allow more outside connectivity to the I&C systems e.g. for external diagnosing purposes, but before this opportunity can be used, there should be a good assurance that threats related to cyber security have been taken care of. The same applies to wireless systems, which in addition carry the possibility of interference with sensitive equipment.

From a process point of view there is a need for smarter logics, protection and interlocks. A solution of these needs may require the creation of a new philosophy for logic control. An intelligent monitoring of sensors to predict wear and tear has been proposed and could be very feasible with decreasing costs of I&C. Finally an increasing number of nuclear I&C projects may increase the volume of the market to provoke I&C vendors to develop new products.

4.5 Cyber security

Cyber security poses a new challenge for computer based system. Cyber security differs from other safety precautions in the respect that it can be seen as the game against an intelligent malevolent counterpart. The simple solution in responding to threats connected to cyber security is isolate the real time I&C from the outer world, but this policy may not be viable in the future. The most feasible strategy of the nuclear industry in creating protection to threats connected to cyber security seems to rely on solutions created in other areas. One problem however, is that nuclear power plants may be considered as interesting targets for various troublemakers and they should therefore be hardened to withstand also advanced attacks.

5. CHALLENGES WITHIN HUMAN FACTORS ENGINEERING

HF engineering is expected to support the design of the HSI in the main control room and in other control stations. Research within the HRP has been very active in this area and many interesting solutions have been proposed. The discussion below brings up a few ideas where R&D has a potential to be fruitful.

5.1 The task of control room operators

The tasks of control room operators have been characterised to consist of 99 % boredom and 1 % sheer terror. This situation has not changed and the characterisation conveys the well known problem of a transfer from normal to disturbed operation. There is still today a large need to support the control room operators in making this transfer and to provide all possible information that can help in handling abnormal events. The integration of diagnosing tools, information displays and procedures can provide help, but concrete solutions are still missing. An additional benefit would be if the systems would be able to support team work in the control room and with a technical support centre.

One target for HF engineering is to present good solutions for how information from the plant can be integrated in terms of important variables, system states, event logs, alarms, etc. It is also important to make it is easy to navigate between different displays and to insert control actions in a logical and consistent way. The general visual oversight and giving operators a process feel are still issues, which have not yet been resolved to a complete satisfaction.

One area, where until now relatively little has been done, is how different HSI solutions can be used to support contacts between the main control room and maintenance activities. The work order systems have already with success been computerised at some plants, but a better integration of information in the control room, in the work order system and in the tag-out handling would still be welcome. One may even consider a specialised control room to support the management of refuelling outages. Easy to use interfaces for the support of recording and archiving functions would also be welcome.

One interesting question, which may warrant new thinking, is to what extent operator time could be utilised during normal operation. If the plant runs steadily at 100 % power the operators may use time for various support activities. One possibility would be to use simulation to give the operators a possibility to ask the question "What's if" e.g. for validating procedures. Simulation could also be used build alarm filtering algorithms, which otherwise tend to become a large engineering effort. One may also ask if it should be allowed for the operators to build their own personalised displays in the control room.

5.2 Utilising new technologies

The challenge in utilising new technologies lies in the possibility to find smarter ways of doing things. In the future one can expect to see a higher level of abstraction in displays, where reference is not given only to single variables, but also to mass and energy flows as well as to system and subsystem states. Situation based displays have been proposed, but their penetration to the plants has so far been minor.

An integration of information in the control room has taken place, but there are still stand alone systems for purposes such as access control, fire protection, radiation protection, HVAC, etc. Decreasing costs of sensors and cabling may make it feasible include additional instrumentation for monitoring valve line-ups and subsystem states to support verification of operational readiness.

Artificial intelligence came with large promises during the 1980ies, but very few real applications have emerged. This failure is understandable, because a system based on a large set of `if_then_else_` rules cannot easily be made transparent for the operators. If the systems instead would build on verified knowledge bases and automatic reasoning algorithms, they would be easier to validate. Such a concept may even move towards the realisation of computerised control room assistants.

5.3 Demonstrating human performance

A large challenge that has to be addressed is how human performance in a given systemic setting can be demonstrated. The common research approach to do statistical comparisons in a large number of experiments is not viable in an industrial environment, because shift operators can seldom be made available to the extent needed. One possibility might be to be able to demonstrate rapid acceptance and learning rates in the operation of a new system. A practical method to validate new HSI could also combine objective performance assessments with subjective evaluations after running a few well selected scenarios.

Another need for demonstrating human performance is connected to the work of the shift as a team in disturbed and emergency situations. In some countries it is even a regulatory requirement that such an assessment of the work skills of the operators as a team is a part of the licensing procedure.

6. I&C AND HF IN A LONGER TERM

Challenges within I&C and HF fields in a longer term will be determined by more general development trends. Presently most I&C and HSI solutions are based on proprietary software, but this situation may change. A transfer to new plants types will take place, but today it is too early to give a prediction of possible

routes to be taken. Present reasoning about safety may also need rethinking, which may bring in new approaches for regulatory oversight.

6.1 Two paradigms of software development

In software development there are presently two competing paradigms, proprietary code and open source. For applications with a very high reliability requirement there is a need to be able to assess both the source code and its development history. A larger adherence to the open source software paradigm may at least in principle make it easier to collect evidence that a specific piece of software is not susceptible to common cause failures and that it can withstand cyber security attacks [10]. The use of software developed under an open source license, may also make it easier to reuse earlier development efforts in consecutive I&C modernisations.

6.2 New plant types

In considering I&C and HF needs in a longer term, there is a need to foresee demands that may arise from the deployment of new reactor types. In comparison with present nuclear technologies, there are four major improvement areas that are seen as objectives for the next generation of reactors. These areas are

- better safety,
- better fuel efficiency,
- better economy,
- better proliferation resistance.

The so called Generation IV International Forum was chartered in 2001 as an international co-operation to address the challenges in developing completely new reactors [11]. So far six main plant concepts have been selected for further development, but also others may be considered. One of the major ideas in the development is that future plants should be integrated as components into the fuel cycle to minimise the produced nuclear waste [12].

The new reactors are expected to be available commercially around 2030, which means that results from R&D should be available in due time before that to allow the necessary engineering to be undertaken. Today it is difficult to predict issues that will emerge and which reactor types will take the lead. It seems however clear that new measurements will be needed. It is also assumed that the automation level of the new plants will be much higher than what is typical today.

6.3 Providing justifications for safety

It is not enough that nuclear power plants are safe, but they have also to provide convincing evidence to regulators and the public that they are safe. This means that methods and tools for building safety have to be supported by similar methods and tools to reason about safety. The ultimate question of "what's safe enough" is still valid and it will still be so for many years to come. The question itself has to be resolved in a political negotiation process in the society, but it would be important that science and research can support this process with views and articulations.

On a more technical level the justifications for safety are built on concepts such as threats, event categories, safety classification and safety functions. One could say that there is an underlying safety philosophy according to which the design base of a nuclear power plant is built. This design base relies still mostly on deterministic principles, in spite of the fact that it has been amended with methods and tools for probabilistic safety assessments. In resolving specific safety questions it sometimes seems that present constructions would need rethinking in their deeper structures.

Efforts to provide actual evidence for safety will always involve modelling, simulation and visualisation. Computerised methods and tools have become available for these purposes at an increasing rate. Still we are far from the ideal that a new plant from the very beginning would be realised as a computer model, which could be visualised and tested in detail before the plant is built. To reach this goal it would be important that model parameters mimic actual construction parameters as close as possible. If such models can be built they would help in verifying and validating design solutions in the I&C and HF, but also in many other fields.

6.4 Regulatory oversight

Regulatory oversight is based on two main principles. Firstly a set of regulatory requirements is built and secondly the regulator is through inspections, assessments and reviews verifying that these requirements are fulfilled. One challenge is connected to the present diversity in regulatory requirements, which makes it difficult to use experience gained for example in the licensing of one specific I&C platform for a similar project in another country. The regulatory requirement that only proven technology should be used may also need certain qualifications.

A challenge closely related to the collection of justifications for safety is connected to the regulatory requirements. How can we be sure that some set of requirements does not contain internal contradictions? How should a system of requirements be managed in order to reflect the technical development? It would also in one way or another be important to recognise that a simple rule fulfilment never can be considered enough to ensure that a plant is safe. Risk informed licensing has been introduced as a solution to some of the problems discussed above [13].

7. CONCLUSIONS

In both I&C and HF engineering there is a need for improved methods and tools for defining requirements and providing evidence that these requirements are fulfilled. The methods should be based on formal models of the design process and the tools should be computer supported. The most difficult question is what can be considered as a sufficient safety. The answer cannot be given on technical grounds, but it has to be based on societal processes in which risks are compared in a broader perspective.

Considering the I&C and HF fields there are many challenges for the future. Weighting the relative importance between these two fields it seems that there are more open questions within I&C than within HF. One reason for seeing fewer problems in the HF area may be connected to the experience that has been collected from earlier control room modernisations, which have generated many useful approaches. The experience collected from I&C modernisations has instead been more scattered and scarce.

The nuclear industry is too small to develop its own solutions and designs. It has therefore to follow what is going on in the I&C and HF fields in other industries and more generally what is going on within the information, computer and telecommunication fields. Innovative applications of ideas and solutions, which are out there, should make it possible for the nuclear industry to have a successful revival.

Picking the three most important challenges to be addressed within the I&C and HF areas by the HRP, my personal choice would be

- to create solutions that would ensure a large reuse of engineering solutions over the life span of the plants,
- to create methods and tools that would support the reasoning about the acceptability of selected solutions,
- to initiate scoping studies that could support an early utilisation of technological opportunities in the I&C and HF fields.

The MTO research of the HRP has encompassed a large span of activities in software reliability, computer support systems, control rooms and human performance. HRP has in this development been able to take the lead in many important development directions. For the years to come it would be important that HRP has an effective ongoing dialogue with their signatories on new needs and opportunities. The more the HRP could be involved in real projects, the better it would be. In the dialogue the HRP has to find a balance between real challenges and suggestions that are nor yet realistic.

8. REFERENCES

[1] IAEA (2006). Nuclear power reactors in the world, Reference Data Series No.2, April.

[2] CEC (2007). Communication from the Commission to the Council and the European Parliament: Nuclear Illustrative Programme, COM(2006) 844 final.

[3] USDOE (2007). Global Nuclear Energy Partnership Strategic Plan, GNEP-167312.

[4] http://www.nrc.gov/

[5] OECD/NEA (2005). Projected costs of generating electricity, 2005 update.

[6] IAEA (2004). Managing Modernization of Nuclear Power Plant Instrumentation and Control Systems, TECDOC-1389.

[7] Björn Wahlström (2005). Risk assessment and safety engineering; applications for computer systems, SAFECOMP 2005, the 24th International Conference on Computer Safety, Reliability and Security, Fredrikstad, Norway.

[8] M. Hecht, H. Hecht (2002). Systems software requirements guidelines; failure descriptions, NUREG/CR-6734, Vol.2.

[9] R.T. Wood et al (2003). Emerging Technologies in Instrumentation and Controls, NUREG/CR-6812.

[10] Olli Ventä, Björn Wahlström (2007). Investigating the case of Open Source applications within nuclear power, EHPG, Storefjell, Norway, 11th – 16th March.

[11] http://www.gen-4.org/

[12] IAEA (2004). Innovative technologies for nuclear fuel cycles and nuclear power, Conference & Symposium Papers, 24/P.

[13] Björn Wahlström (2003). Risk Informed Approaches for Plant Life Management: Regulatory and Industry Perspectives, FISA-2003, 10-12.11.2003, Luxembourg.